HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/748,839	12/27/2000	Ronald M. Smith SR.	POU919970091US2	7967

7590 01/25/2005

IBM Corporation
Intellectual Property Law
2455 South Road (M/S P386)
Poughkeepsie, NY 12601

EXAMINER	
TRUONG, THANHNGA B	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 01/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/748,839	SMITH ET AL.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08/09/2004 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 December 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Taaffe (US 4, 747, 139), and further in view of Glowny et al (US 5, 537, 642).

3. As per claim 1, the limitation of a cryptographic system (see Taaffe, Abstract, Column 4, lines 30-33; Column 9, lines 20-21) having one of a plurality of states, Taaffe discloses a finite state machine FSM (see Column 2, lines 5530, with a plurality of states see Figure 2, Table Column 6 illustrates present and future states and possible transitions), and interactive way for controlling the transition of the system from an existing state to a future state (Column 2, lines 56-67., Column 6, lines 17-44; Column 7, lines 61-65), the central processing unit provides task to the microprocessor (or co-processor) which is programmed as a FSM and the FSM provides updates on those tasks by reporting the status of the tasks (status messages) (Column 7, lines 8-11) discuss the interaction of the CPU with the FSM). The limitation of storing control information specifying permissible future states based on a current state and a requesting authority is taught by Taaffe. In one embodiment Taaffe teaches that the microprocessor which may includes the FSM and encryptor/decryptor (Column 9, lines 20-21) and memory in the form of tables storage for keying information to be used by the encryptor/decryptor (Column 9, line 30), thus the keying information acts as control information for the encryptor/decryptor at the request of the CPU (authority) for changing the state of the data from unencrypted (present state) to encrypted (future state) (Column 7, lines 8-11; lines 63-67). The limitation of receiving a request from the CPU (authority) to change the current state of the cryptographic system the request containing state change information is disclosed by Taaffe (Column 7, line 8-11 - the

CPU and FSM communicate; lines 13-22 - CPU input key sequence and applies it through the 1/0 to the FSM, Column 9, lines 20-21 - the co-processor can then step through states and thus changing its states, Column 7, lines 63-66) to generate keys or to encrypt/decrypt or return keys to the CPU in compliance with its request. Taaffe is silent on the CPU having means to authenticate whether replies originated and further whether the cryptographic system will perform the requests only after it determines the request are indeed from the CPU.

4. Glowny teaches method of generating an authentication security code for message passed between tasks running on a computer system having addressable memory shared by tasks (for example a request by the CPU to the co-processor and the processing of a tasks (change of state) by the co-processor) see Glowny Column 7, lines 12-17. Furthermore, Glowny teaches validating said authentication security code before processing said request (Column 7, lines 48-50., Column 8, line 1; lines 5-6). It would have been obvious to one of ordinary in the ad at the time the invention was made to have modified Taaffe FSM crypto co-processor with the teaching of Glowny of authenticating information being exchanged between processor to prevent an attacker from intercepting or changing commands being processed in route between the processors. Claim 1 is rejected.

5. As per claim 4, the limitation of including a unique query value in the authentication information is disclosed by Glowny (see Column 6, lines 30-44). Claim 4 is rejected.

6. As per claim 5, the storing a unique transaction value (see Glowny, Column 6, lines 7-9 and lines 22-23), including such a value with requests (see Glowny, Column 6, lines 23-24), the request (task) being carried out by validating that the value is contained in the request (Glowny, Column 6, lines 32-33) and finally updating the value (see Glowny, Column 6, line 66-67). Claim 5 is rejected.

7. Claim 12 recites an apparatus for a means plus function for performing claim 1 and is rejected in view of the same prior art of record.

8. Claim 15 recites an apparatus for a means plus function for performing claim 5 and is rejected in view of the same prior art of record.

9. Claims 2-3, 6-11, 13-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Taaffe and Glowny as applied to claim 1 above, and further in view of Schneier Applied Cryptography.

10. As per claim 2 the authentication of information using digital signature. Neither Taaffe nor Glowny authenticate by using a digital signature (Glowny uses a check sum and random number). Schneier teaches the use of the digital signature for authenticating the sender of a message. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified the teaching of Taaffe/Glowny with those of Schneier because digital signature is more difficult to forge, its authenticity is easily recognized, it is not reusable, unalterable and finally repudiated (see Schneier page 35). Claim 2 is rejected.

11. As per claim 3, Taaffe and Glowny are silent on the limitation of storing a private key in the cryptographic system to be used in generating digital signature. Schneier teaches the use of the private key for digital signing documents. It would have been obvious to one of ordinary skill in the art at the time of the invention was made to have modified the teachings of Taaffe/Glowny with those of Schneier because public key encryption is more secure and does not require third parties see Schneier page 37.

12. As per claim 6, the limitation of providing in addition to a random part a sequential part being incremented upon performance of a request. Taale and Glowny are silent on the need for a sequential part to include with the message request. Schneier note that even in a public key system that it is possible for an attacker to modify the order of the messages without decrypting them. Such attacks are called Replay attack (see Schneier page 58-59). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have added such a number with each request to prevent a replay attack. It should be noted that computers assign to each process a pid, that is process id, and such a number is increment for each new request and so it would be sequential. Claim 6 is rejected.

13. As per claim 7, the inclusion of a digital signature as a means of authenticating the sender as part of the message is taught by the Glowny/schneier combination (see claim 2). Claim 7 is rejected.

14. As per claim 8, the further limitation of storing the public key in for the CPU (authority) and using the public key as a means of authenticating is taught by the combination of Glowny (Column 6, lines 7-8) and Schneier (pages 37-38). It would have been obvious for one of ordinary skill in the ad at the time that the invention was made to have combine the ideas of shared memory with authentication using a public key infrastructure because of the security and conveyance (no third parties). Claim 8 is rejected.

15. As per claim 9, the proposed future state (command) is stored in a pending command register. Glowny discusses managing resources (Column 1, lines 34-40) and notes there are three basic types of messages sent between tasks (in this case, the interaction is between a computer and the operator but in more modern computing engines processor to processor). Some of these relate to pending request (mount tape) and thus one of ordinary skill in the ad at the time of the invention would have been motivated to have modified the Glowny's device with a pending command register to hold request until other tasks could be completed, because each operation carried out on a computer requires perhaps nanosecond to complete and if the processor has to wait for the command to be carried out at the time the other task is completed a lost of hundreds of thousands of operations in the process, and thus a pending command register is more efficient. Claim 9 is rejected.

16. As per claim 10, the limitation of the transition from an initial state (of the state machine) to a final state though a series of intermediate states each being authenticated using bits and a signature summary under the control of the CPU (authority) is taught by a combination of Taaffe (transition between intermediate states - Column 7, 63-67), Glowny (the need to authenticate such transitions, Column 6, lines 30-37) and finally Schneier (authentication through digital signature page 35). Such signatures being carried out using single bit operation would have been obvious to one of ordinary skill in the art at the time that the invention was made because a simple yes 1 or no 0 would be all that is needed to proceed to the next state. Claim 10 is rejected.

17. As per claim 11, the limitation of a program storage device readable by a machine, such that the program consists of instruction executable by the machine

performing the process is disclosed by Taaffe (Column 7, lines 30-42) teaches a means of implementing program storage for his invention. Claim 11 is rejected.

18. Claim 13-14 and claims 15-19 recites a means plus function for performing claim 2-3 6-7 9-10 and is rejected in view of the same prior art of record.

Comments

19. The theoretical underpinning of a classical computer processor is that of a finite state machine. It would appear then that any CPU and cryptoprocessor together with memory and standard authentication being performed using for example Schneier's public key digital signature (which would appear to prevent tampering with commands in transit between the two processors) and at least some sequential indicator to prevent a replay attack would satisfy the limitations recited above.

Response to Arguments

20. Applicant's arguments filed August 09, 2004 have been fully considered but they are not persuasive.

Applicant argues that:

"Taaffe does not disclosed applicants' claimed system except for the authentication steps. In applicants' claimed system, the reply provided to an authority in response to a query contains nonsecret state information regarding the current state of the cryptographic system. In Taaffe's system, on the other hand, the state of the FSM must be kept secret to ensure the security of the encryption procedure. The applicant goes on the argue that the internal state of the FSM in Taaffe's system is by design secret, which the CPU can neither ascertain nor change to an arbitrary value. "

Examiner totally disagrees with applicant and maintains that:

The combined teaches of Taaffe and Glowny prevent an attacker from intercepting or changing commands being processed in route between the processors as set forth in independent claims 1 and 12. In addition, Taaffe does teaches only the particular output key word sequence utilized in the encryption need be held secret (which means that some other output key word sequence does not need to be held secret, another word, this kind of output key word sequence can be nonsecret.

Furthermore, that key can be held secret because the key generator 28 (in Figure 1A) is not readily copied, yet the sequences available from key generators can be readily modified, that means these sequences are held nonsecret (column 4, lines 65-67 through column 5, lines 1-2).

Conclusion

21. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100